MICHIGAN CREDIT UNION LEAGUE & AFFILIATES

January 20, 2016

Chairman Anthony Forlini and Members of the House Financial Services Committee

Thank you for the opportunity to provide input on today's hearing regarding the payment security technology commonly known as "chip and PIN". Your attention to the matter of electronic payment security is appreciated and you undoubtedly share our belief that the security of the electronic payments system is of paramount importance. The payments industry continues to develop technology solutions in an effort to further improve data security.

Most recently, payment security took the form of a small chip on new credit and debit cards. This EMV microchip generates a unique, one-time use code for every consumer transaction. This technology helps to prevent some of the most common types of fraud by making it very difficult for hackers to use credit card data to create counterfeit cards. EMV chip cards provide an innovative layer of security that protects consumer information. This chip technology is very expensive, and its implementation into the US market has been steadily increasing over the past several years.

Unfortunately, certain industry groups have been pursuing a narrative that mandating the use of PINs would eliminate fraud and secure the electronic payments system. This approach is concerning. In an area where technology is constantly evolving, focusing on a single technology creates a false sense of security for consumers. In fact, the use of PINs would not have prevented any of the recent data breaches at "Big Box" retailers.

There is not a single technology that is a panacea when working to prevent data breaches, and the payments-related fraud that results from those breaches. Combating threats to the electronic payments system requires multi-layered and flexible solutions that allow innovation that can be directed at securing the system. Some examples of these technologies include encryption, tokenization (used in ApplePay), biometrics, and network-based monitoring. The dynamic nature of the threats made against the system is one reason mandating any specific technology, including "chip and PIN", is not a solution. Further, multiple federal regulators who have studied the issue and reviewed a multitude of technologies, have not identified "chip and PIN" as the answer to the security threats faced by the system today.

The MCUL supports innovative technology solutions to bring greater security to the electronic payments system, including "chip and PIN" and those technologies mentioned before. The banking industry was responsible for the development of PIN technology nearly 50 years ago. The payments industry is fully aware of its uses and limitations, as well as the fact that PIN fraud rates have been increasing. A PIN is a static data point, and if compromised, the data can be utilized fraudulently.

Additionally, since the high-profile 2013 holiday Target breach, numerous retailers have suffered noteworthy breaches. It's important to note that none of these breaches were the result of customers using debit or credit cards without PINs and the breaches would not have been prevented with the use of PINs. As several retailers collect and store the payment card and personal identifying data of their customers for marketing and sales purposes, these business are not subject to the same data security standards as financial institutions. This gap in data security requirements continues to be a leading factor in how these massive breaches have occurred.

For that reason, the MCUL supports comprehensive data breach legislation that would make all parties with access to important consumer information, including payment information to be subject to the same data security standards. Credit unions and other financial institutions are currently subject to strict standards under the Gramm-Leach-Bliley Act, these standards should cover everyone with access to this important information. Additionally, the MCUL supports the ability for financial institutions to communicate with their members to share information regarding a breach, including the details where the breach occurred. And of course there should be shared responsibility for all those involved in the payments system for protecting consumer data. The parties responsible for incurring a breach should bear some of the financial responsibility for making consumers whole.

The MCUL appreciates the opportunity to provide comments on this issue and we thank the committee for holding a hearing on such an important issue. We welcome the opportunity to engage in future discussions should you wish to discuss data security further.

Sincerely,

Kirk Hanna
Vice President of Government Affairs
Michigan Credit Union League & Affiliates